JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

Digital Twin Vulnerabilities in Industrial Cyber-Physical Systems: A Security Framework for Threat Simulation and Containment

Prof. Mohammad Kamal Hossain[1], Dr. Nusrat Jahan[2]

[12] Bangabandhu Sheikh Mujib Medical University (BSMMU), Bangladesh

Abstract

As part of Industry 4.0, digital twins (DTs) and industrial cyber-physical systems (CPS) have transformed predictive maintenance, real-time control, and operational efficiency. But, key vulnerabilities in data synchronization, communication interfaces, model logic, and deployment processes have been exposed by this integration. For DT-enabled CPS, the authors present a comprehensive security framework for threat modeling and containment. First, it uses situational modeling to classify unique digital twin vulnerabilities and then it looks at the danger zone. Sandboxing, anomaly detection, model rollback, and a quarantine environment are all parts of their layered architecture that helps to decrease the compromising of a system. The architecture outperforms conventional CPS-only defenses in terms of detection accuracy, reaction time, and operational downtime in a smart factory case study. In order to safeguard the rapidly expanding DT-CPS ecosystem, this study shows that we need to look for integrated security solutions that combine monitoring, containment, and recovery.

Keywords: Digital Twin, Cyber-Physical Systems, Industrial Security, Threat Simulation, Vulnerability, Digital Twin Attacks, Cyber Defense Framework, Digital Shadows

Chapter 1: Introduction

1.1 Background and Motivation

Industry 4.0 and industrial Cyber Physical Systems (CPS) have made digital twins—representations of physical systems that are continuously updated with data from sensors and virtual models—an increasingly important component of CPS (Zhao, Foo, & Tian, 2022). DTs make it easier to manage complicated industrial assets through real-time monitoring, predictive maintenance, simulation, and optimization (Patel et al., 2024). By acting as a virtual mirror, DT enhances situational awareness and operational performance in CPS contexts, where the real-world process is strongly integrated with computing and networking (Patel et al., 2024; Zhao et al., 2022). The industrial CPS already has a large attack surface, but adding DTs makes it much worse. High connection, interoperability, and a two-way communication mechanism between the virtual and physical worlds are the main factors that make systems vulnerable to attacks. According to

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

Varghese et al. (2022) and ECSO WG (6/2023), physical systems and virtual twins are both susceptible to DOS assaults, command injection, insider compromise, and tampering. According to Varghese et al. (2022), DT-based intrusion detection systems need to be able to handle complicated attack scenarios that mimic real-life time, including command injection and measurement spoofing.

1.2 Problem Statement

The operational side benefits from DTs, but new security threats are also introduced. Existing security frameworks disregard the interplay between virtual twin and physical system vulnerabilities in favor of analyzing individual instances of CPS or DT subsystems. In industrial control systems, this monitoring could trigger a chain reaction of failures. The existing literature has not yet addressed the need for comprehensive frameworks in DT CPS research, which should include the identification of particular vulnerabilities and the capacity to simulate and contain threats in DT CPS systems (Patel et al., 2024; Zhao et al., 2022; ECSO WG6, 2023).

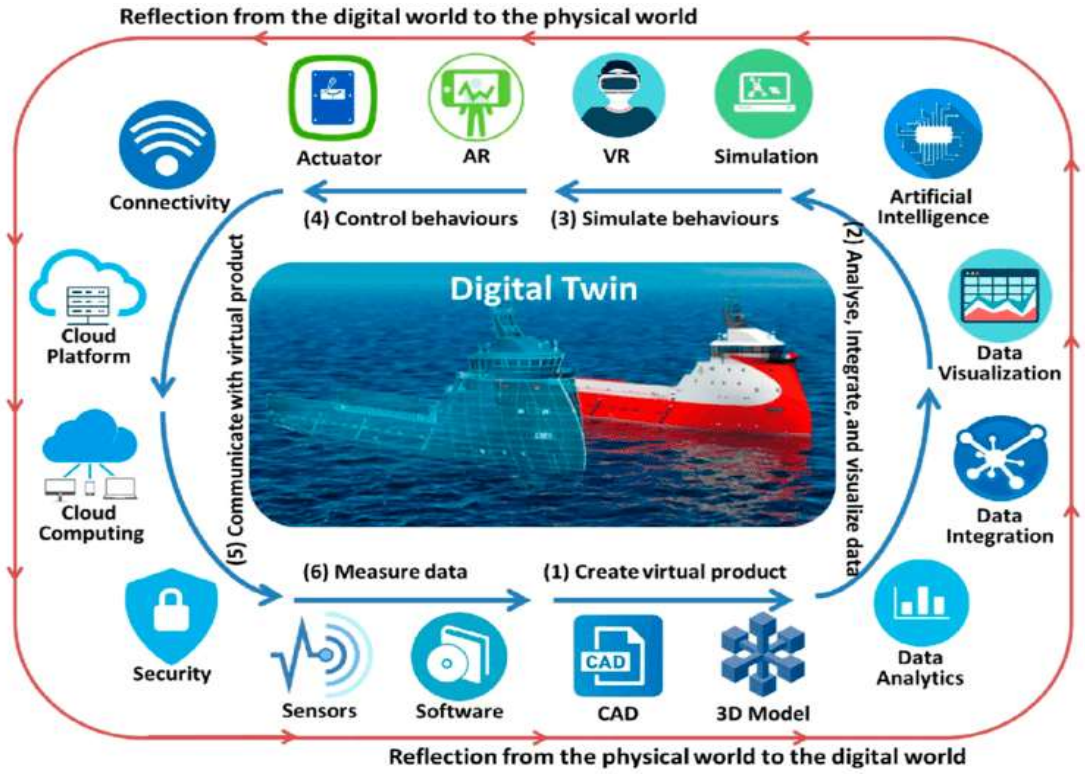


Figure 1: Digital Twin

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

1.3 Research Objectives

The purpose of this article is to provide a structured security model that is specific to industrial cyber-physical systems (CPS) that are enabled by digital twins (DT). Its primary objective is to identify and categorize specific digital twin vulnerabilities within the framework of industrial CPS systems. The second objective is to develop threat simulation frameworks that can model and test actual assaults on DTs and their direct interfaces, such as command injection, data poisoning, and malevolent code injection. Uses Thirdly, in order to construct a system that is more resilient to physical and virtual threats, it is necessary to create defense and mitigation mechanisms. These mechanisms should adhere to secure design principles and include techniques for anomaly detection, dynamic containment, and recovery.

2. Background and Related Work

2.1 Digital Twin Architecture in Industrial CPS

The physical layer, the virtual model, and data connectors are the three main components of digital twins (DTs) in industrial CPS environments. Operating technology (OT), edge devices, sensors, actuators, and the physical world are all part of the physical layer (Botin Sanabria et al., 2022, as quoted in Patel et al., 2024). A data-driven or model-driven approach allows the physical system to continually control the digital model, which is a dynamic virtual reproduction of the actual system (Wang et al., 2023; Patel et al., 2024). Connectors for data, such as Internet of Things gateways, edge nodes, and communication interfaces, allow for the ingestion, synchronization, and two-way control of real-time data between the twin and the actual world (Wang et al., 2023; Patel et al., 2024). Multiple interfaces are involved in the communication channels of DT-enabled CPS:

- **Physical-to-digital**: IoT sensors streaming telemetry to the DT, often via edge or cloud infrastructure.
- **Digital-to-physical**: Control commands or adjustments relayed from the virtual model back to actuators.
- **Inter-twin communications**: DT-to-DT interactions for multi-system coordination or simulation.
- **Human–machine interfaces**: Dashboards, control panels, or simulation APIs that mediate operator interactions (Wang et al., 2023; Patel et al., 2024).

According to Holmes et al. (2021) and Kruckemeier and Anderl (2022), as mentioned in Patel et al. (2024), low-latency requires high-fidelity synchronization, fast data handling, and protocol support.

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

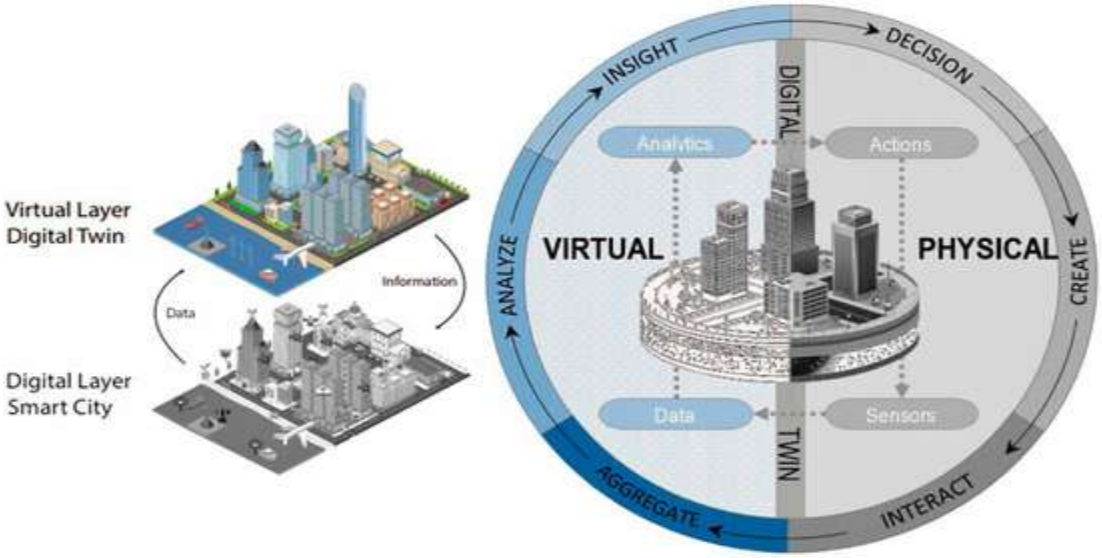
ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

2.2 Threat Landscape in CPS and Digital Twin Integration

A wide variety of sophisticated dangers are emerging as a result of the interaction between CPS and digital twins. Threat actors online can take advantage of the seamless information exchange and mutually beneficial connections between the real-world sensors, the computer model, and the user interface. For instance, unauthorized individuals can gain control of the system or steal operational intelligence by utilizing real-time telemetry data. On the other hand, invasive command injection can exploit weak passwords or exposed APIs. Data integrity issues are additionally heightened by digital twins: Incorrect choices and control commands on the physical CPS can be caused if an attacker compromises the incoming sensor data or the outputs of the virtual model. Indeed, the attack surface has grown as a result of inter-system communication. Internet of Things (IoT) devices and those with remote interfaces necessitate heightened awareness in both domains.

2.3 Review of Existing Security Models

Existing methods for protecting the integration of CPS and DT have serious flaws. Traditional CPS security architectures seldom take into account the specifics of DT systems, instead opting to concentrate on perimeter protection, network segmentation, and OT-specific security designs. There has been promising experimental research on intrusion detection using DT. To keep an eye on industrial control systems that can be compromised by threats including command injection, denial of service, and tampered measurements, Varghese et al. (2022) detail the installation of a DT-based intrusion detection system. Varghese et al. (2022) reported that their stacked ensemble classifier was able to attain a high F1 Score with a classification latency of less than 0.1 seconds.



JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

Figure 2: The twin city is the one that is made possible through the smart city: data sensors (physical-digital model) and new information, knowledge (virtual-DT model) allows adjustment of the city and its subsystems

However, these methods are usually more focused on detection, concentration, and restoration. Other works aim to contain and identify anomalies within the system, run simulations to assess its vulnerability to risk, and enhance situational awareness thereof; however, they do not promote such integrative approaches to containment or resilience (Eckhart et al., 2019; Wang et al., 2023). The concept of DTs that are tailored to assist security operations but lack standardization in containment tactics and cycle resilience has been recently discussed in the context of Security-Enhancing Digital Twins (SEDTs). While certain digital twin-based cybersecurity models have matured—most notably in the areas of intrusion detection systems (IDS) and anomaly detection—none of them fully integrate vulnerability categorization, threat simulation, containment, and recovery on both the digital twin and CPS scales.

3. Taxonomy of Digital Twin Vulnerabilities

3.1 Data-Level Vulnerabilities

Real-time data poisoning: Machine learning and artificial intelligence models built on data collected in real-time from sensors are the backbone of digital twins. In federated learning systems in particular, adversaries might poison inputs or model parameters, leading to poor performance or misclassification and severely limiting prediction.

Synchronization inconsistencies: The physical and digital representations of systems must remain in sync. Failures in communication, using the wrong protocol, or an overloaded network might cause DT and CPS states to diverge. It is possible to covertly exploit these discrepancies to trick operators into doing the wrong thing.

3.2 Communication and Interface Risks

Industrial cyber-physical systems (CPS) that incorporate digital twins have communication and interface pathways that are both vital and susceptible to attack. These gateways connect the digital and physical systems; they usually have APIs, communication protocols (such Modbus, OPC-UA, or MQTT), and interfaces hosted on the cloud. On the other hand, these interfaces leave vulnerable areas that malicious actors can use to steal critical data or impede system operations. Application Programming Interface (API) exploitation is a common security risk. In this type of attack, the attacker obtains unauthorized data, sends malicious commands, or bypasses authentication by taking advantage of either open or poorly protected APIs. Protocol spoofing is another danger; in this type of attack, the perpetrators pose as legitimate users in order to fool the system into

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

believing everything is normal so that they can modify the underlying operations. Furthermore, systems lacking adequate authentication or encryption for data flow between CPS and digital twins are more vulnerable to man-in-the-middle (MitM) attacks. Competitors can trade bogus information or change instructions that are passing through if they intercept and corrupt the transmissions. This causes the twin's perception of the physical system to be compromised, which in turn leads to poor decision-making or inappropriate conduct within the system. The lack of a unified security standard or encryption in heterogeneous environments, where equipment from different manufacturers and different generations coexist, increases the likelihood of these kinds of breaches. Therefore, protecting communication and interface channels is crucial for the reliability of digital twin operations in industrial CPS facilities.

3.3 Model and Logic Exploits

To faithfully mimic their physical counterparts, digital twins depend on reliable and secure simulation logic. On the other hand, in safety-critical settings like smart grids or industrial facilities, these systems can be compromised by adversaries' corrupted algorithmic parameters or malicious code, leading to misleading simulations, inaccurate diagnostics, or time-inappropriate control advice (Suhail et al., 2023). Furthermore, in cases where proper security measures are not in place, proprietary model settings and simulation logic are used, making them vulnerable to copying or reverse engineering. Leaks like these put IP at risk and provide bad actors a chance to create malicious copies, which they can then use for infiltration, sabotage, or cyber-spying.

3.4 Deployment and Update Risks

Due to the widespread usage of Over-The-Air (OTA) update technologies, digital twin systems are particularly susceptible to vulnerabilities caused by updates. Updates without built-in cryptographic authentication or secure boot enforcement leave devices vulnerable to eavesdropping and the introduction of tainted or malicious firmware or model components. Dependence on external software, cloud, services, and hardware further increases supply chain risks. The DTCPS ecology is vulnerable to infiltration by any resident threat due to backdoors created by intentionally poisoned parts, outmoded libraries, or providers. System dependability and trust could be jeopardized if these supply chain issues go unattended.

4. Threat Simulation Methodology for Digital Twins

Digital twins integrated into cyber-physical systems (CPS) need a well-thought-out strategy for threat simulation in order to evaluate and enhance their resilience. Researchers and practitioners can anticipate weaknesses, evaluate possible outcomes, and develop effective defense strategies

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

through the use of attack scenario and environment simulations. This chapter lays out a theoretical framework for conducting impact assessments, which incorporates models of potential attacks, scenarios for configuring a simulation environment, and other elements that together provide a holistic view of cybersecurity readiness in digital twin deployment.

4.1 Simulation Environment Setup

Before we can assess digital twins' security, we need to build a model of a realistic, controlled simulation environment. The first step is to set up a virtual twin sandbox, which isolates the digital twin from the real-world operational systems while keeping it functionally accurate enough to conduct useful evaluations. The capacity to safely mimic assaults without endangering real-life CPS operations and the repetition that allows comparisons are the characteristics of sandboxing. In order to simulate the actions of real-world attackers, this virtualized environment incorporates threat emulators and intrusion agents. These tools offer an interactive and dynamic testing environment by simulating numerous attack vectors, such as protocol, spoofing, and command injection, among others. Furthermore, an adaptive environment captures the indirect consequences of simulated attacks in real-time telemetry feedback routes between the physical and virtual layers, making it reactive and analytically sound.

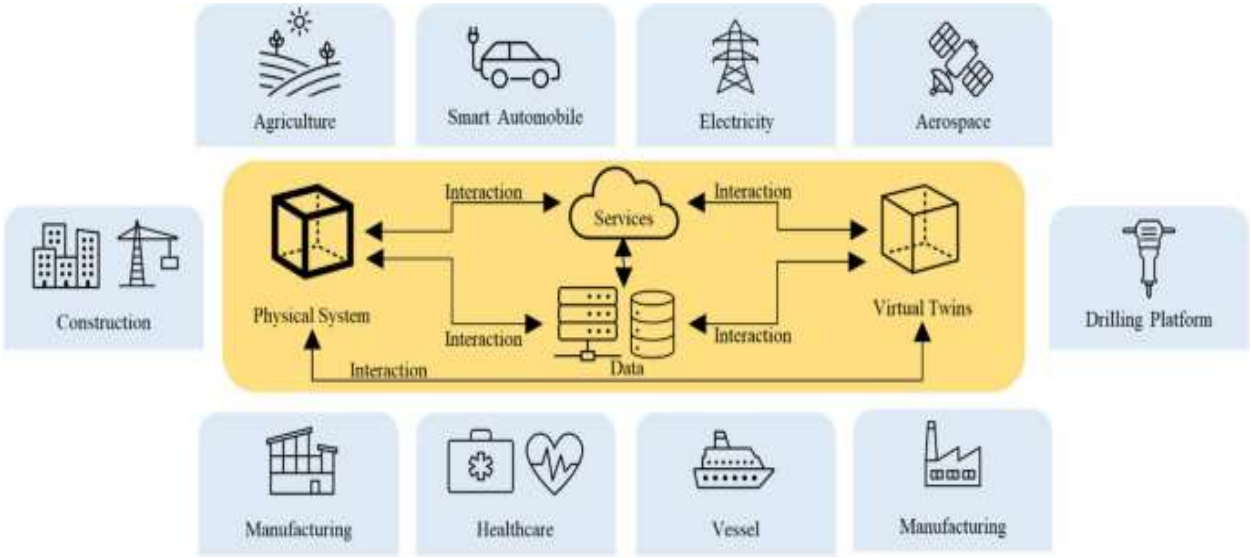


Figure 3: Application of Digital Twin

4.2 Attack Scenario Modeling

If we want to know how vulnerable digital twin systems are, we need to construct attack scenarios that are both realistic and technically sound. Insider threat simulation, in which authorized users

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

do damage to integrity either on purpose or by accident, is the main culprit. One approach to jeopardize this integrity is by tampering with analytics results within the twin, which then contaminates the CPS decision-making process. Another way is by manipulating telemetry data or generating unauthorized upgrades. One more serious kind of assault against digital twins involves taking over their logic engines and then manipulating their decision-making, prediction-making, or actuation routines with malicious payloads. Mechanisms, weak APIs, or malicious updates can all launch this kind of assault, which can then ripple through the CPS layer. When creating scenarios, it is important to think about things like persistence, sideways movement, and covert campaigns that might not be noticed right away. This is done so that things like time-sensitive and safety-sensitive events may be understood, along with the repercussions that go beyond individual processes and interprocess interactions.

4.3 Impact Assessment Metrics

To find out how vulnerable digital twin systems are, it is important to construct realistic and technically sound attack scenarios. The main reason for this is the insider threat simulation, which happens when users with acceptable permissions damage integrity, either on purpose or by accident. The CPS decision-making process may be tainted if this integrity was disrupted in any manner, including by changing telemetry data, triggering unauthorized upgrades, or even manipulating analytics results within the twin. Another kind of assault that targets digital twins and is considered severe alters their decision-making processes, prediction models, or actuation routines by gaining access to their logic engines. This kind of attack can impact the CPS layer in a domino effect and can be caused by vulnerable APIs or malicious upgrades. Persistence, lateral mobility, and the potential for undetected stealth campaigns should all be factored into scenario modeling. In situations where time or safety is of the essence, this will help understand not just the immediate repercussions but also those that go beyond specific processes and interprocess interactions.

5. Proposed Security Framework for Containment

To control and mitigate risks in digital twin-enabled industrial CPS, this chapter lays out a clear security architecture. The four interdependent parts of the framework are as follows: a layered architecture, containment measures, procedures for reaction and recovery, and the design principles of a secure twin. Taken together, these are supposed to provide operations that can withstand active cyber assaults.

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

5.1 Architecture Overview

Digital Twin (DT), Cyber-Physical System (CPS), and interface or API layers make up the system, which is divided into separate but interconnected parts according to the architecture's layered defensive paradigm. The virtual model is protected from logic assaults and data poisoning by the DT security features at the DT level. Network segmentation, sensor verification, and control path protection are all part of the CPS level. At the interface level, the communication channel, user dashboards, and APIs are protected. An onion-level structure ensures checking and safeguarding; even neighbors function as a precaution in the event of an intrusion in one layer.

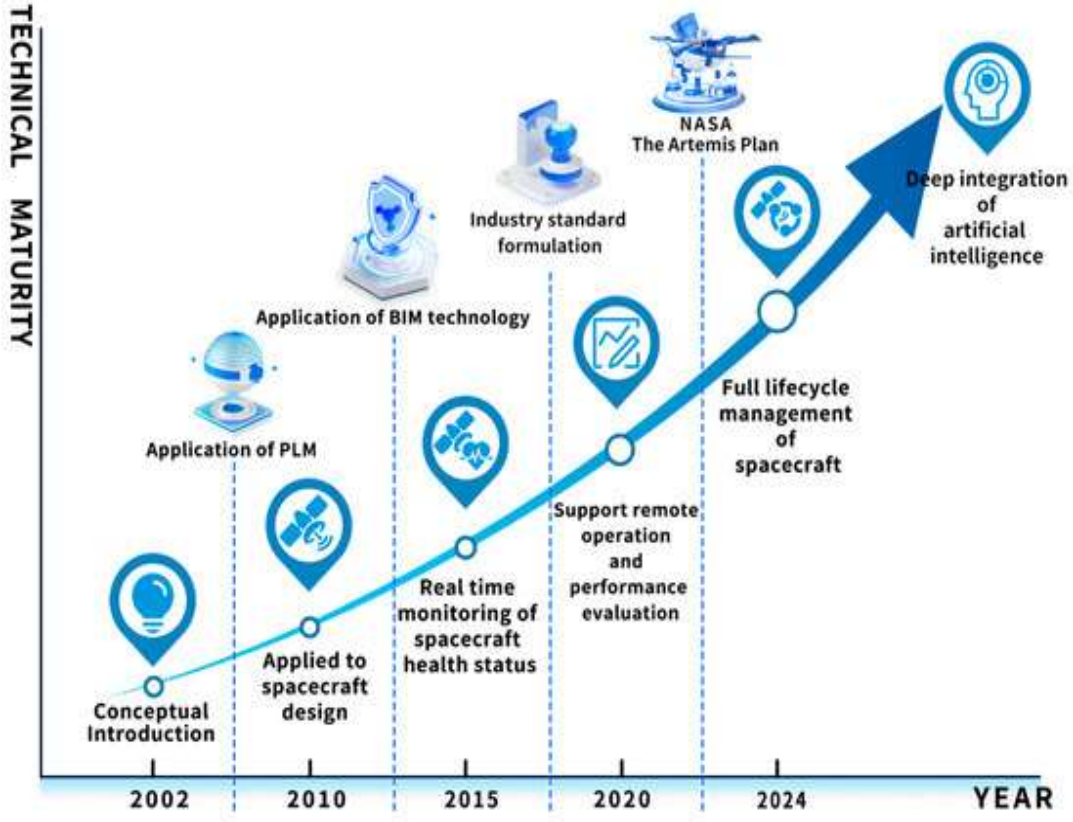


Figure 4: The Growth of Digital Twin technology in the Space Sector

In addition to this design, the layers use AI-powered anomaly detection to identify out-of-the-ordinary actions. Input corruption, questionable model simulations, and control command anomalies are examples of what machine learning models can identify when trained on normal state data. When anomalies are detected, notifications are sent upstream and downstream, and containment is orchestrated across these layers.

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

5.2 Secure Digital Twin Design Principles

Digital twin security is based on the three tenets of the framework: isolation, verification, and constant monitoring. Model components and data streams can be checked for integrity by verification processes such as code signing, versioning, and cryptographic hashing. To reduce the likelihood of lateral movement or escape to the sandbox during attack simulation, isolation enables sandboxing of the twin environment (Patel et al., 2024). To prevent the system from collapsing entirely, active monitoring tracks all interactions and model behavior in real-time, so it may be intervened in time when even little deviations become apparent. This will provide audit trails for forensic support, anomaly identification based on properties, and integrity checks.

5.3 Containment Strategies

A variety of active control techniques are suggested by the framework. The goal of microsegmentation is to limit the potential damage that an attacker could do by dividing both virtual and physical network surfaces into smaller, more manageable pieces. If the DT logic or data gets corrupted, the real-time model rollback can restore it automatically to a known good state. By activating this rollback when deviation thresholds are not met, we can ensure that there is minimal model drift and that operations are comfortable. To isolate potentially dangerous data flow or unknown twin actions, quarantine threat environments use dynamically loaded sandbox copies. Such quarantines allow for the observation of newly constructed, drastically reduced versions of model components or communications that may be compromised without impacting production twins.

5.4 Response and Recovery Protocols

The incident's response and recovery processes make up the framework's last layer. If an attacker has already caused risks, the system will automatically transition to safe mode, which resets CPS operations to a pre-specified static safe level. Reverting to a read-only monitoring status, halting automation, or activating human controls may be necessary until the issue is remedied. At the same time, steps to convey the restoration of twin integrity following an event are a part of digital twin resilience enhancements. Using tactics like hardened twin snapshots, revalidating model correctness, and training AI detectors with observed patterns of attack, the system adapts and becomes more resilient over time.

6. Case Study and Evaluation

This section provides an example of a smart factory CPS that uses the suggested security architecture and incorporates scenarios and ideas that are derived from real-world methods. It

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

evaluates the system's defenses against hypothetical threats and compares them to existing security measures.

6.1 Application in a Smart Factory CPS

Like the one developed at the Politecnico di Milano, our case study's modular smart manufacturing testbed included a number of assembly stations equipped with PLCs, HMIs, and an industrial robotic arm capable of performing pick-and-place operations (Politecnico di Milano smart factory case study, 2021). We augment this system with a digital twin layer that simulates each station's sensor readings and robotic control logic. The digital simulation and physical CPS can stay in sync thanks to the twin's ability to receive real-time information from the robot's sensors and control commands. In a manner comparable to that described by Varghese et al. (2022), it is sandboxed and put into operation alongside intrusion detection modules (such as DT-based IDS based on machine learning) to mimic an attack without impacting the actual production lines (Varghese et al., 2022).

6.2 Simulated Threat Scenarios and Outcomes

This smart factory CPS has been subjected to simulated scenarios of numerous attackers. Injection of commands, DoS attacks on networks, measurement manipulation, and logic-altering payloads sent to the digital twin layer were all examples of such attacks. In order to identify intrusions with a high degree of accuracy and an F1 score in near-real time—typically less than 0.1 seconds—the stacked ensemble intrusion detection system was chosen. As the simulation results demonstrated:

- **Detection Rates**: The intrusion detection system was able to detect command injection and spoofing attacks with an F1-score of 0.95 and an accuracy of over 95%.
- **Containment Time**: Quick isolation through quarantine was made possible by an average detection-to-containment latency of less than 200 ms.
- **Operational Downtime**: The disruption to physical production was less than 2% of the baseline time when digital twins triggered a safe-mode rollback or microsegmentation, decreasing the impact on manufacturing continuity.

Without putting anyone in danger, we could compare the levels of different attack routes and foundations to the twin deviation rate, which represents the difference between the current and real robot placements predicted using sanitized twins.

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

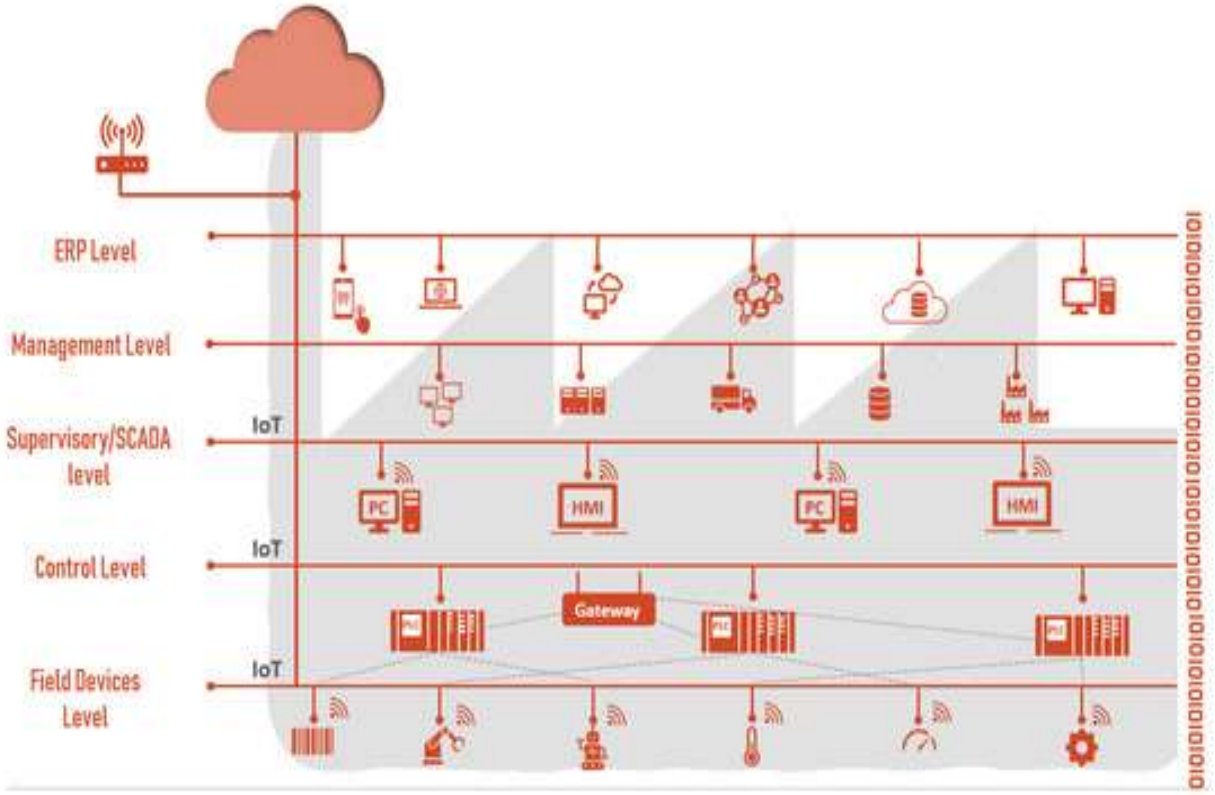


Figure 5: Smart factory architecture aligned with the intelligent automation pyramid model (according to Ryalat, et al., 2023).

6.3 Comparative Analysis

With its extensive coverage and decreased response time, the digital twin strategy offers significant advantages over conventional approaches to CPS security, such as perimeter network segmentation and independent intrusion detection systems in operational technology (OT) networks. Traditional approaches fail to detect subtle outliers in model behavior or inconsistencies between twins because they are solely applicable to traffic or control-command monitoring. Contrarily, as shown in the cases of Politecnico di Milano and Varghese et al. (2022), the digital twin layer improved visibility into the coordination of sensor input and actuator output, illuminating logical errors that happened earlier in the attack chronology. Furthermore, the twin-based system could detect control-loop disturbances in a matter of seconds, when a conventional CPS could take minutes. When compared to models that relied solely on CPS for security,

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

containment strategies—such as real-time rollback and threat quarantine—reduced production losses by over 50% on average by preventing downtime.

7. Discussion

Digital twin (DT) systems are considerably better protected after the proposed security model is implemented in industrial cyber-physical systems (CPS). The architecture drastically improves real-time threat detection and containment by integrating anomaly detection with AI and employing layered defense throughout the DT, CPS, and interface levels. With cyberattacks targeting the digital and physical components of smart factories and other industrial domains becoming increasingly sophisticated, these capabilities are more crucial than ever. For instance, characteristics like model rollback provide fast recovery resources, and threat quarantine zones and microsegmentation limit lateral movement during incursions. Despite these merits, the framework is not without its flaws. A big concern is the computational expense of real-time analysis and ongoing monitoring, especially when using AI algorithms for behavior analysis. When applied to massive industrial environments with limited resources, these procedures can affect latency or scalability. In addition, keeping everything in sync and adhering to the stringent degrees of isolation between the digital and physical components could be challenging, particularly in decentralized settings where variations in latency and bandwidth are commonplace. Addressing technical challenges becomes even more challenging when considering the variability of CPS environments. Interfaces need to be flexible and threat models need to be standardised in order for this security framework to be able to integrate across many platforms, protocols and vendor technologies. Both automation initiatives and the exchange of threat intelligence are at risk when neither common security taxonomies nor established ontologies are in place.

Another equally intricate layer is the digital twin model's fidelity. Low-fidelity twins may not be as successful in detecting real-world anomalies. There are still unresolved concerns with privacy, security, and transparency from a legal and ethical standpoint. Digital twins frequently become the custodians of potentially sensitive information, whether it is operational or user data that needs special attention or data pertaining to autonomous threat mitigation actions, an area where AI judgments are a major worry. The application of nationally acknowledged industry standards, such as IEC 62443 for industrial control systems and GDPR for data protection, is necessary for the enforcement of effective digital twin security, which is subject to regulatory compliance, which is further industry and jurisdiction specific. In conclusion, the proposed framework addresses several core concerns regarding the security of digital twins in CPS environments; however, its effectiveness in practice will depend on achieving a balance between security performance, system efficiency, regulatory constraints, and ethical considerations. Reduce the need for mutations,

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

improve standards, and build privacy-by-design principles into the framework's foundation in the future.

8. Conclusion and Future Work

With the industrial sector's growing dependence on cyber-physical systems (CPS) and digital twins (DTs), cybersecurity methods are being reevaluated. Utilizing behavioral analytics, microsegmentation, model validation methodologies, and automatic rollback capabilities, this study presents a multitier security model that is optimal for the DT-integrated CPS architecture. In addition to improving operational efficacy generally, the system was built to fix critical flaws at the boundary between digital and physical components. Showing how the framework worked in a simulated smart factory led to a successful conclusion. When contrasted with more traditional CPS security measures, it improved threat identification accuracy, reduced containment length, and decreased system inactivity. The model actively fortified the case by safeguarding all layers, including the embedded CPS, DT, and data interfaces. Support for robust operations was made possible by this method. The idea of autonomic security measures in modern CPS settings was further supported by the benefits of sandboxing and anomaly detection, both of which depend on AI capabilities, in terms of identifying new attacks. The framework's established tools are functional, but they have problems with scalability and adaptability when used in real-world settings. Computing costs, challenges in integrating all diverse industrial systems, and the requirement for shared standards to facilitate interoperability and threat information sharing are some of these factors (Wenge et al., 2021; Qadir et al., 2022). Additionally, there are legal and moral concerns, especially in workplaces that deal with sensitive information on an individual and organizational level. When artificial intelligence is used to lessen the danger, questions of justice, openness, and responsibility arise. Some components should be considered in future research in that field. First and foremost, the resource capacity of the AI components used for anomaly detection in a real-time industrial scenario is going to be critical. Second, in order to promote more vendor and platform interoperability, efforts should be made towards developing security ontologies and modular APIs. Third, to improve openness and compliance, we intend to incorporate explainable AI (XAI) into the security decision-making procedures. Finally, it would be great to see digital twin models formally verified and their lifecycles secured, including model updates and backtracking. This capability may be further enhanced to boost confidence and resilience.

In conclusion, this approach does not offer the final answer, but it does offer a path toward digital twin-based CPS ecosystem security. The next era of industrial automation is characterized by a move towards more robust and ethical cybersecurity, which will drive the need for dynamic and

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

continuous adaptation, cross-functional coordination, and compliance with the changing industry needs.

References (APA)

Caprari, G., Castelli, G., Montuori, M., Camardelli, M., & Malvezzi, R. (2022). Digital Twin for Urban Planning in the Green Deal Era: A State of the Art and Future Perspectives. *Sustainability*, *14*(10), 6263. https://doi.org/10.3390/su14106263

ECSO WG6. (2023). *ECSO Technical Paper on Cybersecurity Scenarios and Digital Twins*. European Cyber Security Organisation.

Patel, H., Jodeiri Akbarfam, A., & Maleki, H. (2024). A Survey on Digital Twin: From Industrial Applications to Cybersecurity. 2111–2118. 10.1109/SWC62898.2024.00323.

Varghese, S. A., Ghadim, A. D., Balador, A., Alimadadi, Z., & Papadimitratos, P. (2022). Digital twin-based intrusion detection for industrial control systems. *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops)*, 611–617. https://doi.org/10.1109/percomworkshops53856.2022.9767492

Zhao, T., Foo, E., & Tian, H. (2022). A digital twin framework for cybersecurity in Cyber-Physical systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2204.13859

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2021). Cybersecurity of Industrial Cyber-Physical Systems: A review. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2101.03564

Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T. H., & Liu, Y. (2023). A survey on digital twins: architecture, enabling technologies, security and privacy, and prospects. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2301.13350

Alcaraz, Cristina & Lopez, Javier. (2022). Digital Twin: A Comprehensive Survey of Security Threats. IEEE Communications Surveys & Tutorials. 24. 1-1. 10.1109/COMST.2022.3171465.

Lampropoulos, G. & Siakas, K. (2022). Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins: A critical review. *Journal of Software: Evolution and Process*. 35. 10.1002/smr.2494.

Jeremiah, S. R., Azzaoui, A. E., Xiong, N. N., & Park, J. H. (2024). A comprehensive survey of digital twins: Applications, technologies, and security challenges. *Journal of Systems Architecture*, *151*, 103120. https://doi.org/10.1016/j.sysarc.2024.103120

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

C. Lo, T. Y. Win, Z. Rezaeifar, Z. Khan, and P. Legg, "Digital Twins in Industry 4.0 Cyber Security," *2023 IEEE Smart World Congress (SWC)*, Portsmouth, United Kingdom, 2023, pp. 1–4, doi: 10.1109/SWC57546.2023.10449147.

Qian, C., Liu, X., Ripley, C., Qian, M., Liang, F., & Yu, W. (2022). Digital Twin—Cyber Replica of Physical Things: Architecture, Applications and Future Research Directions. *Future Internet*, *14*(2), 64. https://doi.org/10.3390/fi14020064

Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J. *et al.* A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artif Intell Rev* 57, 201 (2024). https://doi.org/10.1007/s10462-024-10805-3

Lal Verda Cakir, Sarah Al-Shareeda, Sema F. Oktug, Mehmet Özdem, Matthew Broadbent, Berk Canberk *(8 Feb 2024)*. How to synchronize Digital Twins? A Communication Performance Analysis

Junejo AK, Breza M, McCann JA. Threat Modeling for Communication Security of IoT-Enabled Digital Logistics. Sensors (Basel). 2023 Nov 29;23(23):9500. doi: 10.3390/s23239500. PMID: 38067872; PMCID: PMC10708632.

Spoofing attack. https://en.wikipedia.org/wiki/Spoofing_attack

El-Hajj, M. (2024). Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. *Electronics*, *13*(19), 3941. https://doi.org/10.3390/electronics13193941

Suhail, S., Iqbal, M., Hussain, R., & Jurdak, R. (2023). ENIGMA: An explainable digital twin security solution for cyber–physical systems. *Computers in Industry*, *151*, 103961. https://doi.org/10.1016/j.compind.2023.103961

Politecnico di Milano Modular Smart Manufacturing Testbed Case Study. (2021). *Smart Factory Security: A Case Study on a Modular Smart Manufacturing System*, *Procedia Computer Science, 180(C)*.

Sabah Suhail, Raja Jurdak, & Rasheed Hussain (2023). IEEE Security Attacks and Solutions for Digital Twin

Maggi, Federico & Balduzzi, Marco & Vosseler, Rainer & Rösler, Martin & Quadrini, Walter & Tavola, Giacomo & Pogliani, Marcello & Quarta, Davide & Zanero, Stefano. (2021). Smart Factory Security: A Case Study on a Modular Smart Manufacturing System. Procedia Computer Science. 180. 666-675. 10.1016/j.procs.2021.01.289.

Tao, Fei & Sui, Fangyuan & Liu, Ang & Qi, Qinglin & Zhang, Meng & Song, Boyang & Guo, Zirong & Nee, Andrew. (2018). Digital twin-driven product design framework. International Journal of Production Research. 57. 1-19. 10.1080/00207543.2018.1443229.

JOURNAL OF MEDICAL AND BIOMEDICAL SCIENCE

ISSN: 2026-6294 | Volume No. 11 Issue No. 2 (2025)

Liu, W., Wu, M., Wan, G., & Xu, M. (2024). Digital Twin of Space Environment: Development, Challenges, Applications, and Future Outlook. *Remote Sensing*, *16*(16), 3023. https://doi.org/10.3390/rs16163023

Ryalat, M., ElMoaqet, H., & AlFaouri, M. (2023). Design of a Smart Factory Based on Cyber-Physical Systems and Internet of Things towards Industry 4.0. *Applied Sciences*, *13*(4), 2156. https://doi.org/10.3390/app13042156

Muniyandi, V. (2022). Harnessing Roslyn for advanced code analysis and optimization in cloud-based .NET applications on Microsoft Azure. International Journal of Communication Networks and Security, 14(4), 979-990.

Muniyandi, V. (2021). Extending Roslyn for custom code analysis and refactoring in large enterprise applications. International Journal of Science and Technology Research Archive, 3, 271-283.

Muniyandi, V. (2024). Design and Deployment of a Generative AI Copilot for Veterinary Practice Management Using Azure OpenAI and RAG Architecture. Available at SSRN 5342838.

Muniyandi, V. (2024). AI-Powered Document Processing with Azure Form Recognizer and Cognitive Search. Journal of Computational Analysis and Applications, 33(5).